UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/288,462	04/08/1999	RICHARD ALEXANDER HARRINGTON	777.222US1	7531

22801 7590 08/23/2006

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 08/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/288,462
Filing Date: April 08, 1999
Appellant(s): HARRINGTON ET AL.

Allan T. Sponseller
Reg. No. 38,318
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 05 June 2006 appealing from the Office action mailed 01 July 2005.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is substantially correct. The changes are as follows:

Claims 1-4, 6, and 8 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Rubin, U.S. Patent No. 5,530,752, in view of Yoshida, U.S. Patent No. 6,075,862, in view of Chan, U.S. Patent No. 6,473,860, in view of Davis, 6,058,478, and further in view of Patel, U.S. Patent No. 6,192,474.

Claim 5 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Rubin, in view of Yoshida, in view of Chan, in view of Davis, in view of Patel, and in further view of Scott, U.S. Patent No. 5,199,073.

Claim 7 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Rubin, in view of Yoshida, in view of Chan, in view of Davis, in view of Patel, and in further view of Elgamal, U.S. Patent No. 5,825,890.

These grounds of rejection were required in response to Appellant's after-final amendment, filed 01 December 2005, which amended claim 1 to incorporate the elements of claim 35, and amended claim 2 to incorporate the elements of claim 36. Claims 35 and 36 were rejected under 35 U.S.C. §103(a) as being unpatentable over Rubin, in view of Yoshida, in view of Chan, in view of Davis, and further in view of Patel, in the final office action mailed 01 July 2005. No new grounds of rejection exist because all of the claim limitations where fully addressed in the final office action mailed 01 July 2005.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,530,752	RUBIN	6-1996
6,075,862	YOSHIDA	6-2000
6,473,860	CHAN	10-2002
6,058,478	DAVIS	5-2000
6,192,474	PATEL	2-2001
5,825,890	ELGAMAL	10-1998

5,199,073 SCOTT 3-1993

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

Claims 1-4, 6, 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rubin, U.S. Patent No. 5,530,752, in view of Yoshida, U.S. Patent No. 6,075,862, in view of Chan, U.S. Patent No. 6,473,860, in view of Davis, U.S. Patent No. 6,058,478, and further in view of Patel, U.S. Patent, No. 6,192,474. Referring to claims 1-3, 8, Rubin discloses a protected software system wherein software is delivered encrypted in a software package (Col. 5, lines 6-30), which meets the limitation of an encrypted software module, with a decryption key (Fig. 3, 305), which meets the limitation of a decryption key to decrypt the encrypted software module, and a version number of the software module (Fig. 3, 303), which meets the limitation of a database containing identification of trigger files and including decryption keys. In order for the user to obtain access to the encrypted software, the transformer (setup program)(Col. 6, lines 2-6), which meets the limitation of an executive for using the decryption key to decrypt the encrypted software module, reads the version number from the Executable Object Code System Program to identify what program the user is licensed to use (Col. 6, lines 25-53), which meets the limitation at least one of a set of trigger files is stored on a computing system, wherein each of the trigger files indicates authorization to install the encrypted software module. Rubin does not disclose the software package containing multiple versions of software programs. Yoshida discloses a software distribution system wherein a software package contains a demonstration version and a full version that is encrypted. If the user does not have the proper authorization to access the full

version then the demonstration version is installed. If the user subsequent obtains proper authorization then the full-encrypted version is decrypted and installed on the users terminal (Col. 2, lines 6-55), which meets the limitations of loading a different version of the software module onto the computing system when the trigger file is not stored on the computing system, determining which version of the software module to install, wherein the different versions have different threshold encryption strengths. Yoshida does not disclose encrypting both the demonstration version and the full version of the software program using different encryption strengths. Chan discloses an information distribution system wherein software programs included in a distribution package (Col. 1, lines 41-53) can be encrypted separately using different encryption strengths (Col. 6, lines 50-60). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the protected software system of Rubin to have software packages with multiple versions in them wherein each version is encrypted with a different encryption strength in order for the software vendor to save on cost required for production and distribution of individual software packages as taught in Yoshida (Col. 2, lines 6-9) and to help the software providers match the requirements of many information providers (Chan, Col. 2, lines 18-22) as well as to provide a flexible encryption method (Chan, Col. 2, lines 24-28). Rubin does not disclose encrypting the decryption key. Davis discloses an encrypted public key through the use of a private key (Col. 3, lines 55-59). It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the decryption key in the protected software system of Rubin in order to authenticate the sender of the information as taught in Davis (Col. 3, lines 60-64). Davis does not disclose using a hash value as an encryption key. Patel discloses using the hash of authentication information as

an encryption key (Col. 2, lines 37-59). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a hash value as an encryption key in Davis in order to add security prior to establishing the key as taught in Patel (Col. 3, lines 36-38).

Referring to claim 4, Rubin does not disclose encrypting the decryption key. Davis discloses an encrypted public key through the use of a private key (Col. 3, lines 55-59). It would have been obvious to one of ordinary skill in the art at the time the invention was made to encrypt the decryption key in the protected software system of Rubin in order to authenticate the sender of the information as taught in Davis (Col. 3, lines 60-64).

Referring to claim 6, Rubin does not disclose that the encrypted software module is a cryptographic software module. Davis discloses storing cryptographic programs (Abstract). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the encrypted programs of Rubin to be cryptographic programs because there are restrictions on the use and distribution of cryptographic technology, as taught in Davis (Col. 1, lines 31-51), so the protected software system of Rubin would be ideal to control who has access to these cryptographic programs.

Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rubin, U.S. Patent No. 5,530,752, in view of Yoshida, U.S. Patent No. 6,075,862, in view of Chan, U.S. Patent No. 6,473,860, in view of Davis, U.S. Patent No. 6,058,478, and further in view of Patel, U.S. Patent, No. 6,192,474 as applied to claims 1, 2 above, and further in view of Scott, U.S. Patent N. 5,199,073. Referring to claim 5, Rubin does not disclose generating hash values for each decryption key in the database. Scott discloses generating a hash value from the key value corresponding to database addresses (Col. 1, lines 11-16 & Col. 2, lines 3-10). It would have

been obvious to one of ordinary skill in the art at the time the invention was made to generate hash values in the databases of Rubin for the decryption keys because the generation of hash values is a technique used in many areas of data processing and data encryption as taught in Scott (Col. 1, lines 11-16).

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rubin, U.S. Patent No. 5,530,752, in view of Yoshida, U.S. Patent No. 6,075,862, in view of Chan, U.S. Patent No. 6,473,860, in view of Davis, U.S. Patent No. 6,058,478, and further in view of Patel, U.S. Patent, No. 6,192,474 as applied to claims 1, 6 above, and further in view of Elgamal, U.S. Patent No. 5,825,890. Referring to claim 7, Davis does not disclose the cryptographic programs being dynamic link libraries (DLL) for providing a secure socket layer (SLL). Elgamal discloses applications that employ a Winsock DLL in conjunction with the SLL library (Col. 12, lines 30-34). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the cryptographic programs of Davis to employ dynamic link libraries in conjunction with a secure socket layer library in order to achieve a high security communication line in the application program as taught in Elgamal (Col. 12, lines 34-48).

(10) Response to Argument

Before addressing Appellant's arguments, the combination of references will be fully explained (with respect to claim 1) along with the motivations for their respective combination.

Rubin discloses a protected software system wherein encrypted software is delivered in a software package (Col. 5, lines 6-30), which meets the limitation of an encrypted software module that is a first version of the software. The software package contains a decryption key (Fig. 3, 305 & Col. 5, lines 30, 38-42 & Col. 7, lines 10-20), which meets the limitation of a

decryption key to decrypt the encrypted software module. The software package also contains a version number of the software module (Fig. 3, 303 & Col. 5, lines 28-30). In order for the user to obtain access to the encrypted software (i.e. decrypt), the transformer (setup program)(Col. 6, lines 2-6), reads the version number from the Executable Object Code System Program to identify what program the user is licensed to use (Col. 6, lines 25-53), which meets the limitation of an executive for using the decryption key to decrypt the encrypted software module when at least one of a set of trigger files is stored on a computing system and to install the first version of the software module on the computing system when at least one of the set of trigger files is stored on the computing system. The transformer will compare previously access version numbers (i.e. stored version numbers) with the version number of the encrypted software package to determine if the user can access the software package (Col. 6, lines 36-56), which meets the limitation of wherein each of the trigger files indicates authorization to install the encrypted software module.

Rubin does not disclose the software package containing multiple versions of software programs (claimed second version of the software module). Yoshida discloses a software distribution system wherein a software package contains a demonstration version and a full version that is encrypted. If the user does not have the proper authorization to access the full version then the demonstration version is installed. If the user subsequent obtains proper authorization then the full-encrypted version is decrypted and installed on the users terminal (Col. 2, lines 6-55), which meets the limitations of wherein a second version of the software module is installed if at least one of the set of trigger files is not stored on the computing system.

It would have been obvious to one of ordinary skill in the art at the time the invention was made for the protected software system of Rubin to have software packages with multiple versions in them in order for the software vendor to save on cost required for production and distribution of individual software packages as taught in Yoshida (Col. 2, lines 6-9). Otherwise the distributors would have to produce individual software packages for each software module, which would become costly in comparison.

Yoshida does not disclose encrypting both the demonstration version and the full version of the software program using different encryption strengths. Chan discloses an information distribution system wherein software programs included in a distribution package (Col. 1, lines 41-53) can be encrypted separately using different encryption strengths (Col. 6, lines 50-60), which meets the limitation of a first version of the software module uses greater than a threshold strength encryption, and a second version of the software module uses a strength encryption that is not greater than the threshold strength. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the protected software system of Rubin to have software packages with multiple versions in them wherein each version is encrypted with a different encryption strength in order to help the software providers match the requirements of many information providers (Chan, Col. 2, lines 18-22) as well as to provide a flexible encryption method (Chan, Col. 2, lines 24-28). Such flexibility would be desired when considering the computation power needed for certain levels of decryption (Chan, Col. 6, lines 56-60).

Rubin does not disclose encrypting the decryption key. Davis discloses an encrypted public key through the use of a private key (Col. 3, lines 55-59). It would have been obvious to

one of ordinary skill in the art at the time the invention was made to encrypt the decryption key in the protected software system of Rubin in order to authenticate the sender of the information as taught in Davis (Col. 3, lines 60-64).

Davis does not disclose using a hash value as an encryption key. Patel discloses using the hash of authentication information as an encryption key (Col. 2, lines 37-59)(the authentication information in Rubin is the version number or claimed trigger file), which meets the limitation of the decryption key is encrypted as a function of a cryptographic hash value produced by hashing a corresponding trigger file with a hash algorithm. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use a hash value as an encryption key in Davis in order to add security prior to establishing the key as taught in Patel (Col. 3, lines 36-38).

Appellant's argument that "the mere discussion of using a hash of a value calculated as a part of Diffie-Hellman Encrypted Key Exchange as a session key in Patel '474 does not provide any disclosure or suggestion of hashing the version number of Rubin, much less of using the resulting hash value to encrypt a decryption key," is not persuasive because Patel discloses using the hash of authentication information as an encryption key. The **only** authentication information used in Rubin is the version number (See Col. 6, lines 36-56 of Rubin, which describes how previously access version numbers of software are compared with current version numbers of software to determine if the user can access the software with the current version number). Motivations for using the hash value as an encryption key, and encrypting a decryption key with an encryption key are provided above.333

Applicant's argument that "the Office's basis and supporting rationale for the §103(a) rejection is not supported by the teaching of the cited references" is not persuasive because the

rejection, discussed above, provides motivation directly from the cited references to support the combination of the cited references.

Appellant's argument that "there still is no assertion that a hash value is produced by hashing a corresponding trigger file as recited in claim 1," is not persuasive in view of the preceding paragraph.

Appellant's arguments (appeal brief pages 9-10) with respect to Yoshida, Chan, and Davis mirror the previous arguments and have been fully addressed above.

Appellant's arguments with respect to claims 2 and 3, also mirror the previous arguments and have been fully addressed above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Benjamin E. Lanier

Conferees:

Kim Vu

Christopher Revak

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100